SCENARIO

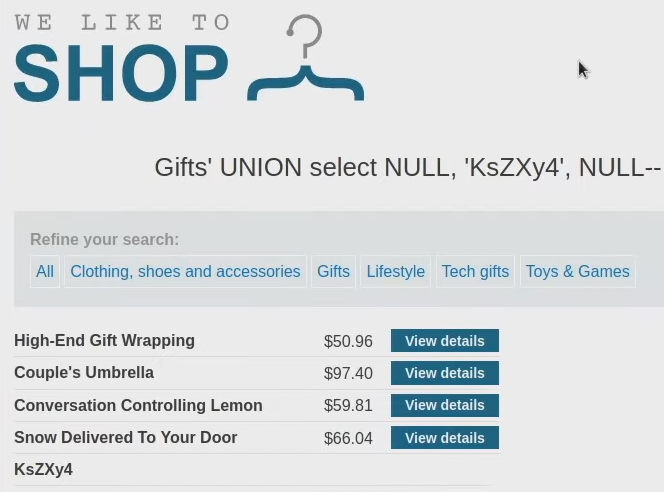
The product category filter in the application is not secure against SQL injection. Our goal is to utilize a UNION attack to harvest usernames and passwords from the users table, enabling unauthorized access.

**PROCEDURE**

1. Initiate Burp Suite and grab the request that fiddles with the product category filter.
2. Confirm that the query returns two columns with '+UNION+SELECT+'abc','def'--.
3. Adjust the payload to fetch user credentials from the users table.

**PAYLOAD**

'+UNION+SELECT+username,+password+FROM+users--

**PROOF OF CONCEPT**

**REMEDIATION**

1. Apply multi-factor authentication for database access.
2. Ensure web applications have no direct access to the database, but instead access it through a middle layer.
3. Ensure that database error messages are generic, not revealing any sensitive information or the internal structure.
4. Use stored procedures to encapsulate the logic for accessing the database.
5. Conduct regular vulnerability assessments and penetration tests to discover and rectify potential vulnerabilities.